SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES AND ACCESS TO JPL CONTROLLED FACILITIES

[CT, FP-NR&D, FP-R&D, CIS, LH-T&M, T&MC, FPC, CREI, A-E – 05/08] [NPR 2810.1A 05/06; FAR 52.204-9]

(a) The subcontractor shall be responsible for Information Technology security for all systems connected to a JPL network or operated by the subcontractor for JPL, regardless of location. This clause is applicable to all or any part of the subcontract that includes information technology resources or services in which the subcontractor must have physical or electronic access to sensitive information contained in unclassified systems that directly support the mission of JPL. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

(2) Acquisition, transmission or analysis of data owned by JPL with significant replacement cost should the subcontractor's copy be corrupted; and

(3) Access to JPL networks or computers at a level beyond that granted the general public (e.g. bypassing a firewall).

(b) The subcontractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this subcontract. The plan shall describe those parts of the subcontract to which this clause applies.

(c) Within 90 days after subcontract award, the subcontractor shall submit an IT certified and accredited Security Plan (see SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems), that addresses the security of its IT assets connected to the "JPL network", e.g., (jpl.nasa.gov domain). This plan must be developed using the tools and databases provided by JPL's Office of the CIO, and be consistent with and further detail the approach contained in the subcontractor's proposal or sealed bid that resulted in the award of this subcontract and in compliance with the requirements stated in this Article.

(d) In addition to complying with any functional and technical security requirements set forth in the schedule and the provisions of this subcontract, the subcontractor shall request NASA Personal Identity Verification (PIV) Credentials for its personnel who require regular, unescorted, or unsupervised physical access to JPL. Subcontractor personnel will not be granted unescorted physical to JPL until they have been approved for and issued a PIV Credential. In addition, the subcontractor shall obtain unique electronic identifications (from the JPL Office of the CIO) for its personnel that need electronic access to JPL systems, programs, and data.

(e) The subcontractor's personnel, including grantees, research associates, co-op students, and all foreign nationals (including permanent resident aliens), requiring continuing and official unescorted access to NASA facilities, buildings or have access to the internal "JPL network", shall be screened per JPL procedures. Subcontractor personnel WILL NOT be authorized access to NASA facilities, buildings, or sensitive information without submission of the PIV Credential required investigative documentation to the JPL Office of Protective Services AND a favorable access determination by NASA Security Officials based upon their review of the following investigative paperwork; and the results of a Office of Personnel Management (OPM) Background Investigation.

(1) JPL's Office of Protective Services (OPS) Initiation Form

Office of Personnel Management (OPM) Standard Form (SF) 85P (SF – 85P), Questionnaire for Public Trust Positions/BI, and the OPM Optional Form (OF) 306. (f) IT Security Requirements: The requirements stated in JPL D-7155, titled, "JPL Information Technology Security Requirements" (incorporated by reference) apply to all IT assets having an IP address belonging to the "JPL network", e.g., ("jpl.nasa.gov" domain) Compliance with these requirements will be monitored by network vulnerability scans and physical audits as required by the JPL Chief Information Security Officer.

(g) Controlled Facilities: JPL facilities, as defined by the NASA Mission Essential Infrastructure Protection Program (MEIPP) (incorporated by reference), are designated as NASA controlled facilities.

(h) Requirements for Background Investigations:

(1) All subcontractor personnel assigned to JPL (in excess of fifteen (15) days) for computer system administration, computer system maintenance (hardware and/or software), network operation, or have access to restricted areas information, must submit completed PIV documentation to the JPL Office of Protective Services prior to reporting for work at JPL.

(2) All subcontractor personnel requiring access to controlled facilities must deliver completed Personnel Security Clearance (PCL) investigation documentation (SF -86) to the JPL Office of Protective Services prior to being granted access to those controlled facilities. (3) PIV and PCL investigations require original proof of identification, and U.S. citizenship and eligibility for employment. Subcontractor personnel with existing PIV or PCL clearance investigations current within the last five years are not required to submit PIV or PCL investigation documentation forms. The subcontractor must submit a Classified Visit Request for each individual who will be accessing a controlled facility or information system.

(i) Security Incident Reporting: Reportable security incidents are defined in “JPL Information Technology Security Incident Investigation and Reporting Manual (D-7973)” (incorporated by reference). The subcontractor shall promptly call the JPL Help Desk, (818) 354-4357, about any suspected or detected IT security incidents occurring on any IT assets belonging to the “JPL network”, e.g., (jpl.nasa.gov domain).(j) Access:

(1) As a NASA restricted facility, JPL requires that all personnel possess valid identification for unescorted access. Individuals who access JPL on a one-time or infrequent basis are processed as visitors. All visitors are processed through the Visitor Control Center and must possess a valid picture ID issued from a recognized government agency or business organization. All non-U.S. born citizens must possess the original proof of citizenship. All visits by foreign nationals must be approved in advance, and the visitor must possess their original passport or visa as proof of identification and legal status.

(2) Individuals who access JPL on a regular basis for business related activities but do not occupy JPL office space may be provided a PIV Credential. The PIV Credential allows the individual to access JPL through any security-staffed entry gate and allows parking in any outside lot including the Visitor Lot. Prior to the individual receiving this Credential, the subcontractor’s subcontracts manager must submit JPL Form E2190, “Affiliate Start/Separation Notice,” to the JPL Office of Protective Services; and, the subcontractor’s personnel must be approved for the PIV Credential.

(3) The subcontractor shall afford NASA and JPL access to subcontractor facilities, installations, operations, documentation, databases and personnel used in performance of the subcontract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA or JPL data or to the function of computer systems operated on behalf of NASA or JPL, and to preserve evidence of computer crime.

(k) The subcontractor shall notify the JPL subcontracts manager no later than the end of the day of the termination for cause of an authorized subcontractor personnel’s access. The Subcontractor shall notify the JPL Subcontracts manager and the designated JPL Contract Technical Manager no later than ten days after authorized subcontractor personnel no longer require access for any other type of termination. PIV Credential and any other JPL/NASA assets possessed by the terminated subcontractor employee will be retrieved by the subcontractor prior to the departure of the subcontractor employee from the work site. The PIV Credential and property will be turned in to the JPL Office of Protective Services within 24 hours after termination by the subcontractor. Verbal notifications of termination action will be confirmed in writing within 30 days.

(l) The subcontractor must ensure that any forms required for Background Investigations are completed by the individuals who are to perform work under this subcontract as requested by JPL in order to determine eligibility for access to sensitive material or controlled facilities.

(m) Incorporated documents are available through the “Miscellaneous Subcontractor Documents” link on the JPL Acquisition Home Page at the following URL: http://acquisition.jpl.nasa.gov/e2000.htm

(n) The subcontractor shall ensure that its employees, in performance of the subcontract, receive annual IT Security Training in IT Security policies, procedures, computer ethics, and best practices.

(o) The subcontractor shall accept the documents in Table 1 below as “Guidelines”. The subcontractor will place particular emphasis on the documents showing asterisks before the text in Table 1.

TABLE 1

Subcontractor's Use	NPR 2810.1A NIST SP or FIPS Reference
Guidelines	**** FIPS 199 Standards for Security Categorization of Federal Information and Information Systems***
Guidelines	FIPS 140-2 Security Requirements for Cryptographic Modules
Guidelines	FIPS 46.3 Data Encryption Standard
Guidelines	FIPS 201.1 Personal Identity Verification (PIV) of Federal Employees and Contractors
Guidelines	SP 800-12, An Introduction to Computer Security: The NIST Handbook
Guidelines	SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
Guidelines	SP 800-16 IT Security Training Requirements: A Role- and Performance-Based Model
Guidelines	**** SP 800-18 Guide for Developing Security Plans for IT Systems***
Guidelines	SP 800-19, Mobile Agent Security
Guidelines	SP 800-26 Security Self-Assessment Guide for Information Technology Systems
Guidelines	SP 800-27 Engineering Principles for IT Security
Guidelines	SP 800-28 Guidelines on Active Content and Mobile Code
Guidelines	**** SP 800-30, Risk Management Guide for Information Technology System***
Guidelines	SP 800-31 Intrusion Detection Systems
Guidelines	**** SP 800-34 Contingency Planning Guide for Information Technology Systems***
Guidelines	SP 800-35 Guide to IT Security Services
Guidelines	SP 800-36 Guide to Selecting Information Technology Security Products
Guidelines	**** SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems.***
Guidelines	SP 800-41 Guides on Firewalls and Firewall Policy
Guidelines	SP 800-42 Guideline on Network Security Testing
Guidelines	SP 800-44 Guidelines on Securing Public Web Servers
Guidelines	SP 800-45 Guidelines on Electronic Mail Security
Guidelines	SP 800-46 Telecommuting and Broadband Communications
Guidelines	SP 800-47 Security Guide for Interconnecting Information Technology Systems
Guidelines	SP 800-48 Wireless Network Security 802.11, Bluetooth and Handheld Devices
Guidelines	SP 800-50 Building an Information Technology Security Awareness and Training Program
Guidelines	****SP 800-53 Recommended Security Controls for Federal Information Systems***
Guidelines	SP 800-55 Security Metrics Guide for IT Systems
Guidelines	**** SP 800-60 Volume I and II, Guide for Mapping Types of Information and Information to Security Categories***
Guidelines	SP 800-61 Computer Security Incident Handling Guide
Guidelines	**** SP 800-64 Considerations in the Information System Development Life Cycle***
Guidelines	SP 800-65 Integrating Security into the Capital Planning and Investment Control Program
Guidelines	SP 800-77 Guide to IP Sec VPNs